

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----x
UNITED STATES OF AMERICA,

12 CR 301(ADS)

-against-

DECLARATION

DANIEL GREENBERG,
Defendant.

-----x

LARRY E. DANIEL hereby declares the following to be true under penalty of perjury and pursuant to Title 28, United States Code, §1746:

1) I am a digital forensic examiner and part owner of a business known as YourTechnician.com, Inc. DBA Guardian Digital Forensics. I am based in Raleigh, North Carolina.

2) My professional CV is attached hereto as Exhibit A. I started my career working with personal computers in 1982. I have thirty (30) years of experience in troubleshooting, networking, administration, programming and repair of computers starting with MS DOS 1.3. In 2001, I expanded my services to computer forensics. I have more than 200 hours of training specifically in computer and cell phone forensics. I have worked over 500 cases, including death penalty cases, child pornography and sex crime cases, wrongful death, terrorism, homicide, kidnapping, Ponzi schemes, fraud, civil cases and domestic cases. I have testified as an expert witness twenty one (23) times. I am a Digital Forensic Certified Practitioner, an Encase Certified Examiner, an Access Data Certified Examiner, a Blackthorn 2 Certified Examiner and a Certified Telecommunications Network Specialist. I am a published author in the digital forensic field including multiple articles published as well as the co-author of the book, "Digital Forensics for Legal Professionals, Syngress 2011. I have presented over 50 times at technical and legal conferences. I am an Associate Member of the National Association of

Criminal Defense Attorneys and a member of the Consortium of Digital Forensic Specialists and the Digital Forensics Certification Board.

3) I have been retained by the defendant herein, through the Criminal Justice Act, to conduct a forensic examination of certain computer data contained on images of computers which I understand to have been created by a contractor for the Federal Trade Commission in or about the summer of 2009. The data was recently turned over to the defense by the Government in this case.

4) I have reviewed the forensic images of hard drives and forensic images of logical data where hard drives could not be fully copied, as well as the notes provided by the persons performing the forensic copying of the computers and hard drives, turned over to the defense by the government, which was provided on a portable hard drive. I have not been able to access all of the data provided, primarily due to the method used by the Government's contractor to collect the forensic copies as well as the failure of the Government's contractor to properly verify that the data could be accessed prior to leaving the collection site.

5) Some of the forensic copies are from servers that have multiple hard drives configured in a RAID arrangement, which is a configuration of two or three separate hard drives installed in a server computer. The server hardware makes the arrangement look like one single hard drive when accessing the drives. Some server computers are configured in such a way that the forensic copies of the multiple hard drives cannot be reconstructed back into the "single" hard drive to get to the data which was viewable when the server computer was in operation.

7) It is common practice to make what is known as a "Logical Image" of data contained on complex systems (such as server computers in RAID configurations or network attached storage (NAS) devices) as a backup, along

with the physical acquisitions. Basically, this captures all of the data on the server computer and ignores the complexities of the RAID configuration, thereby assuring that all of the data is useable, accessible, and in proper working order. It is important to note that making a logical image takes significantly less time than a full physical acquisition.

8) According to FTC-DE Worksheet IT02, this forensic copy should be of the VIZNETIC database. I am told that VIZNETIC is a customer service program. FTC-DE Worksheet IT02 includes the following information:

“Server Name: VIZNETIC-73099. Photos indicate server times were consistent with local date and time. Unable to complete forensic image due to power failure and time constraints; logical capture of potential evidence performed instead. Could not complete capture of some items, namely image (picture) files.”

Therefore, the government was aware that they had not successfully copied this drive.

9) The same analysis applies to the drive labeled FTC-DE IT04 . The Worksheet connected with that drive includes the following information:

“Server Name: DEV2. Photos (see folder 104) indicate server times were consistent with local date and time. EnCase images files are from imaging jobs that were interrupted during a power failure and are incomplete. A logical copy of data from the system drive was not performed. Originally, using FTK Imager, each logical drive (C, D, and F) was to be its own image.”

Therefore, the government was aware that the copy was incomplete and had not successfully copied this drive.

10) Similarly, FTC-DE Worksheet IT06 includes the following information:

“Unable to access file system directly via USB or Ethernet. All attempts at logical data acquisition via network shares (share name: CC-NAS; with 3 folders of interest) were unsuccessful. FTK Imager Lite may have produced partial FTK logical image files. Unit's LCD display indicated 493 GB of 676 GB of storage was available. Network IP address via DHCP: 192.168.132.66.”

Therefore, the government was aware that they had not successfully copied

this drive.

11) According to FTC-DE Worksheet IT07, this forensic copy should be of the SQL server. FTC-DE Worksheet IT07 includes the following information: "Server Name: Dumbledore. Photos indicate server times were consistent with local date and time. Server had no USB ports. Data was acquired logically via network share connections from a separate PC (the IT 'administration' workstation). Data was collected from 4 share locations and organized into subdirectories: IT07-1 through IT07-4."

This drive was also not successfully copied. In the case of this computer, the contractor did not attempt to copy any of the SQL server files, which are critical to this case as the SQL server database contained all of the customer transactions.

12) The web sites that were actually in use at the time would have resided on a specific kind of server called a web server. I have not found any of the web server data at this point, nor have I found any of the SQL Server databases that I need to determine the customer history and interaction with Classic Closeouts. It is likely that the SQL Server databases and the web server data is contained on one of the computer servers in RAID configuration that I have been unable to rebuild at this point in time, or they were not copied at all, which at this point, I believe is the most likely scenario.

13) Based upon the information provided to me and my forensic examination of the drives, as noted, it is likely that the original computer drives and servers contained significant quantities of data, including customer service emails, which are now inaccessible due to the improper imaging of the drives by the Government's contractor, and such data is now unrecoverable and unusable in the absence of the original computer drives.

DATED: RALEIGH, NORTH CAROLINA

May 15, 2013



LARRY E. DANIEL